AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method to facilitate global timeout in a distributed computing environment, comprising:

receiving an access request from a user at an application in the distributed computing environment;

determining if the distributed computing environment has issued an authentication to a user device through which the user accesses the application, wherein the authentication is stored within a time-stamped token on the user-device, and ~~wherein~~ determining if the authentication has not expired by comparing a time within the time-stamped token against a current time; and

if the authentication has not been received or has expired, redirecting the access request to a single sign-on server for the distributed computing environment;

otherwise granting access to the application to the user.

2. (Original) The method of claim 1, wherein the distributed computing environment includes multiple partner applications distributed across multiple network servers coupled to a public network.

3. (Original) The method of claim 2, wherein the public network includes the Internet.

4. (Currently amended) The method of ~~claim 2~~claim 1, wherein determining if the distributed computing environment has issued the authentication to the user involves:

receiving an authentication credential from the user;

verifying that the authentication credential is valid; and

providing the time-stamped token to the user-device, wherein the time-stamped token includes the authentication and a time.

5. (Original) The method of claim 4, wherein determining if the authentication has expired involves:

recovering the time-stamped token from the user-device;

adding the specified period to the time within the time-stamped token to produce an expiry time; and

detecting if a current time is later than the expiry time, whereby if the current time is later than the expiry time, the authentication has expired.

6. (Original) The method of claim 5, wherein the time within the time-stamped token is updated to the current time by a partner application when the partner application is accessed.

7. (Original) The method of claim 4, wherein the time-stamped token is a domain cookie, wherein the domain cookie is accessible by multiple network servers within a domain on the public network.

8. (Original) The method of claim 4, wherein the time-stamped token is encrypted to prevent attacks.

9. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method to facilitate global timeout in a distributed computing environment, wherein the computer readable storage medium includes one of a volatile memory and a non-volatile memory, the method comprising:

receiving an access request from a user at an application in the distributed computing environment;

determining if the distributed computing environment has issued an authentication to a user device through which the user accesses the application, wherein the authentication is stored within a time-stamped token on the user-device, and ~~wherein~~ determining if the authentication has not expired by comparing a time within the time-stamped token against a current time; and

if the authentication has not been received or has expired, redirecting the access request to a single sign-on server for the distributed computing environment;

otherwise granting access to the application to the user.

10. (Original) The computer-readable storage medium of claim 9, wherein the distributed computing environment includes multiple partner applications distributed across multiple network servers coupled to a public network.

11. (Original) The computer-readable storage medium of claim 10, wherein the public network includes the Internet.

12. (Currently amended) The computer-readable storage medium of ~~claim 10~~claim 9, wherein determining if the distributed computing environment has issued the authentication to the user involves:

receiving an authentication credential from the user;

verifying that the authentication credential is valid; and

providing the time-stamped token to the user-device, wherein the time-stamped token includes the authentication and a time.

13. (Original) The computer-readable storage medium of claim 12, wherein determining if the authentication has expired involves:

recovering the time-stamped token from the user-device;

adding the specified period to the time within the time-stamped token to produce an expiry time; and

detecting if a current time is later than the expiry time, whereby if the current time is later than the expiry time, the authentication has expired.

14. (Original) The computer-readable storage medium of claim 13, wherein the time within the time-stamped token is updated to the current time by a partner application when the partner application is accessed.

15. (Original) The computer-readable storage medium of claim 12, wherein the time-stamped token is a domain cookie, wherein the domain cookie is accessible by multiple network servers within a domain on the public network.

16. (Original) The computer-readable storage medium of claim 12, wherein the time-stamped token is encrypted to prevent attacks.

17. (Currently amended) An apparatus to facilitate global timeout in a distributed computing environment, comprising:

a receiving mechanism that is configured to receive an access request from a user at an application in the distributed computing environment;

a determining mechanism that is configured to determine if the distributed computing environment has issued an authentication to a user device through which the user accesses the application, wherein the authentication is stored within a time-stamped token on the user-device, and ~~wherein~~ determine if the authentication has not expired by comparing a time within the time-stamped token against a current time; and

a redirecting mechanism that is configured to redirect the access request to a single sign-on server for the distributed computing environment if the authentication has not been received or has expired.

18. (Original) The apparatus of claim 17, wherein the distributed computing environment includes multiple partner applications distributed across multiple network servers coupled to a public network.

19. (Original) The apparatus of claim 18, wherein the public network includes the Internet.

20. (Currently amended) The apparatus of ~~claim 18~~claim 17, wherein the receiving mechanism is further configured to receive an authentication credential from the user, the apparatus further comprising:

a verifying mechanism that is configured to verify that the authentication credential is valid; and

a time-stamp mechanism that is configured to provide the time-stamped token to the user-device, wherein the time-stamped token includes the authentication and a time.

21. (Original) The apparatus of claim 20, further comprising:

a recovering mechanism that is configured to recover the time-stamped token from the user-device;

an adding mechanism that is configured to produce the specified period to the time within the time-stamped token to produce an expiry time; and

a detecting mechanism that is configured to detect if a current time is later than the expiry time, whereby if the current time is later than the expiry time, the authentication has expired.

22. (Original) The apparatus of claim 21, wherein the time within the time-stamped token is updated to the current time by a partner application when the partner application is accessed.

23. (Original) The apparatus of claim 20, wherein the time-stamped token is a domain cookie, wherein the domain cookie is accessible by multiple network servers within a domain on the public network.

24. (Original) The apparatus of claim 20, wherein the time-stamped token is encrypted to prevent attacks.